Heitor Gouvêa

Cybersecurity Researcher and Bug Bounty Hunter

376, Av. João Erbolato, Vila Castelo Branco, Campinas - São Paulo, Brazil
(19) 991 891 355
hi@heitorgouvea.me

SUMMARY

I am an Cybersecurity Researcher and Bug Bounty Hunter, working on projects that help people, organizations and companies take control of their own security.

My work is focused on understanding threat models, analyzing existing applications and building intelligent tools to combat current and future security risk for both individuals or groups.

I have audited high profile websites for security vulnerabilities and have managed and worked in teams of software developers and computer scientists delivering high security architectures.

I have experience developing in a wide array of programming languages including: Shell Script, JavaScript, Perl and Mojo Framework.

I have knowledge of telecommunication and internet protocols including, but not limited to: TCP/IP, UDP, HTTP, FTP, SSH, SMTP and Telnet.

When I am not doing any of that stuff I run a range of open source software projects: https://github.com/GouveaHeitor

EXPERIENCE

Security and Development Analyst

12/2017 - PRESENT

Horizon Four

I acted providing consulting in the field of information security offensive to institutions, private companies and governmental organizations. My work was focused on writing business proposal models, confidentiality and reports, and understanding threat models, analyzing existing applications and building intelligent tools to combat current and future security risk for both individuals or groups. In addition to ministering trainings about Information Security like: awareness, tools and techniques.

Information Technology Trainee

04/2016 - 11/2017

IMA - Computer Associates Municipalities S/A

I participated in the trainee program in order to be trained and prepared to assume strategic positions in the future. During the trainee process I worked directly with clients understanding their problems and later proposing some solutions, developing, performing vulnerability analyzes and maintaining Government Systems that used technologies like: PHP 7, Symfony Framework, JavaScript, CoffeeScript, Doctrine, MySQL, Twig, Ruby On Rails and others technologies..

CERTIFICATIONS

OSCP - Offensive Security Certified Professional - Candidate

A certified offensive security professional is someone who has been able to demonstrate their expertise in penetration testing techniques and tools.

TECHNICAL SKILLS

Application Security: Hardening, Cryptography, Cryptanalysis, Vulnerability analysis, Penetration testing, Code review, Iptables and ModSecurity

Network: TCP/IP, UDP, HTTP, FTP, SSH, SMTP and Telnet

Architecture: Scalability, Distributed system, Decentralized systems, High architecture, Parallel computing and Design patterns

Front-end: HTML5, CSS3, MaterializeCSS, Sass, JavaScript, ReactJS and ReduxJS

Back-end: Shell Script, Perl and Mojo Framework

Database: MySQL and PostgreSQL

Mobile development: PWA

Tools: Bower, Git, Npm, Jekyll, Grunt and Docker

Agile Methods: Scrum and Extreme Programming

Others: Web performance, SEO, Responsive Design, Cross-browser, OOP, UML and Linux Administration

LANGUAGES

Portuguese: native proficiency

English: limited working proficiency